The General Data Protection Regulation and associated legislation

Part 4: FAQs for Community Pharmacy

Version 1: 25th March 2018

Community Pharmacy
GDPR Working Party

Contents

Introduction

1. What is the GDPR and why is 25th May 2018 important?

The General Data Protection Regulation (GDPR) is European legislation that will be directly effective in the UK from 25th May 2018. It will be accompanied by UK specific legislation, a new Data Protection Act 2018 (currently a Bill), which will complement and clarify aspects of the GDPR. It will continue to apply after Brexit.

While the GDPR will bring changes to the way in which data protection is managed, it is more **evolution than revolution**. It makes mandatory what up until now has been considered good or best practice. The basic principles of processing personal data remain broadly the same, although the meaning of personal data is broadened, which may mean that some information is now personal data that previously was not considered to be personal data.

Pharmacy businesses must comply with Information Governance (IG) requirements already, as part of their terms of service with NHS England, and must complete an annual self-assessment, the IG Toolkit. The GDPR builds on these requirements and in 2019 the IG Toolkit will be revised to include GDPR. What you do now will assist you with the 2018/19 IG Toolkit.

2. What is personal data and what are the main terms I need to know?

Key aspects of the GDPR to understand are:

Data subject means the identified or identifiable living individual to whom **personal data** relates.

Personal data includes any information relating to an identified or identifiable natural person (the data subject) who can be identified directly or indirectly (for example, by an NHS number).

Special category personal data is that 'revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, **data concerning health** or data concerning a natural person's sex life or sexual orientation.'

Data concerning health means personal data relating to the physical or mental health of an individual, including the provision of health care services, which reveals information about his or her health status

The GDPR applies to the processing of **personal data** (which may be by automated means) which forms part of a **filing system** or is intended to form a part of a filing system.

A **filing system** means any structured set of personal data which may be accessible according to specific criteria (e.g. name or address) whether centralised, decentralised or dispersed on a functional or geographical basis. So, a pharmacy company's filing system for patients may be in each pharmacy or one system spread across many pharmacies).

The **data controller** determines the purposes and means of **processing** of personal data and there can be joint controllers for certain purposes. The pharmacy company is a controller, processing personal data.

Processing includes, for example, the collection, recording, organisation, adaption, structuring, storage, use and disclosure of personal data. Dispensing a prescription involves processing a patient's data.

The **data controller** of the personal data determines the purposes and means of processing of personal data and there can be joint controllers for certain purposes. The pharmacy business is a data controller, processing personal data

A **processor** is somebody external to the pharmacy who processes personal data on your behalf (as the controller), who you instruct exactly how to process the personal data, for example, a payroll processing company.

The meaning of personal data is now broader and includes data from which natural persons can be identified indirectly. This means that if the information you process can be matched at a later stage with other information (that you hold or somebody else holds) to identify a natural person, it is personal data even though you cannot see to whom it relates. The GDPR refers to this data as **pseudonymised data** – personal data that can no longer be attributed to a specific natural person without the use of additional information. **Pseudonymisation** of personal data is encouraged in appropriate circumstances where those processing some of the data do not to see all of it, for example, removing patient details for pharmacy accounting purposes.

3. Does the GDPR apply to all personal data?

No. The GDPR applies to the processing of **personal data** (which may be by automated means) which forms part of a **filing system** or is intended to form a part of a filing system (see the means of these terms in the answer to question 2).

The GDPR does not apply to the processing of personal data by a natural person in the course of purely personal or household activity.

4. Who's responsible for GDPR and what needs to be done?

Generally, the legal owner of the pharmacy – e.g. the contractor – will be the person responsible for the orgnaisation's compliance with the GDPR. In GDPR terms this person is the data controller. Responsibility for compliance with GDPR cannot be delegated to any one person in the organisation, but one or more persons may be asked to lead one or more projects associated with GDPR – take certain responsibilities – and each person will be accountable for their actions. The data controller also has some responsibility for any other person processing personal data on its behalf (a data processor).

The term 'accountability' is used in the GDPR to indicate that organisations must be accountable – must demonstrate – that they comply with the principles of data protection when processing personal data.

5. Where can I find more information about the GDPR?

More information about the GDPR is available from the:

Information Commissioner's Office (IGO)
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

And

NHS Digital's Information Governance Alliance (IGA)
https://www.digital.nhs.uk/article/1414/General-Data-Protection-Regulation-guidance

Processing personal data

6. What does 'accountability' mean in the GDPR?

The GDPR requires active and demonstrable compliance with data protection principles. Under the Data Protection Act 1998, which is being replaced, compliance was required but did not need to be demonstrated until perhaps a problem, for example, a data breach occurred. The GDPR requires a pro-active, quality assurance approach to data protection and recognition that you must take steps to protect personal data and keep it secure.

For pharmacies, this will mean that records must be kept of the activities on an ongoing basis. This is not a record of everything undertaken, rather a record of classes of processing demonstrating adherence to the principles relating to the processing of personal data. (See Template C in the **Community Pharmacy Workbook** (Part 3)).

7. What records of processing activity do I need to keep?

You must be able to demonstrate that you are processing personal data in accordance with these principles. This will require you to keep records of the activities you undertake and show that you have considered whether the activity complies with each of the requirements.

The data protection principles are largely the same as those under the existing legislation, but under the GDPR, you must now show that you are complying with them. You also need to be able to show that you are processing data lawfully. (See Template C in the **Community Pharmacy Workbook** (Part 3)).

8. What are the data protection principles to follow when processing personal data?

The GDPR requires you to follow certain data protection principles which, briefly, are:

a) processed lawfully, fairly and in a transparent manner;
b) collected for specified, explicit and legitimate purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

9. What is the lawful basis for processing the personal data?

Article 6 of the GDPR sets out how personal data may be processed lawfully:

> *'Article 6 Lawfulness of processing*
> *1. Processing shall be lawful only if and to the extent that at least one of the following applies:*

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

……'

Category 1(b) (c) (d) and (e) are all likely to apply in certain circumstances, but the most appropriate is likely to be 1 (c) – the terms of service for NHS pharmacies and 1(e) – for all pharmacies. The provision of pharmaceutical services by pharmacy businesses is carried out in the public interest, both within the NHS and in the private sector. It is suggested that 1(e) is the most appropriate because this will encompass all pharmacy activities for the provision of healthcare and the management of the NHS, including non-Community Pharmacy Contractual Fretwork (CPCF) activities such as home delivery for 'bricks and mortar' community pharmacies and locally commissioned services.

By a quirk of legislation (unless this is reversed in the UK legislation accompanying the GDPR) pharmacy contractors with the NHS are considered to be public authorities and, therefore, cannot use lawful processing category 1(f) for the provision of pharmaceutical services.

Please note there is another hurdle or consideration if you want to process special categories of personal data lawfully.

10. What is special category data and what does this mean?

Special categories of personal data – those described in Article 9 of the GDPR – may not be processed except for specified purposes also set out in Article 9 and sometimes subject to special conditions.

Special categories of personal data that may not be processed unless there is a specific exception are:

… personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic

> *data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation...*

Therefore, as may be expected data concerning health is a special category of data and it has a specific meaning as follows:

> *'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status*

Data concerning health and other special categories of data may be processed where:

> *(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis,* ***the provision of health or social care or treatment or the management of health or social care systems*** *and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in* ***paragraph 3***

Paragraph 3, as referenced above, **as added to by the new Data Protection Act**, requires that a healthcare professional (such as a pharmacist or a pharmacy technician subject to registration and regulatory oversight e.g. as per the Pharmacy Order 2010), social work professional or a person with a duty of confidentiality under a legal provision, must be responsible for the processing.

11. How do the two hurdles of lawful processing and special category data fit together for data concerning health?

The GDPR has a two-stage process for you to confirm that you have a lawful basis for any personal data you process.

First stage
The first stage is to identify which of several broad categories applies to the personal data you process. These are listed in Article 6 of the GDPR, which is above in the answer to question 8. Data concerning health may be processed because it is necessary for a task carried out in the public interest (Article 6(e)).

If the personal data is not special category data (see Article 6 of the GDPR and question 8 above), the data may be processed lawfully, and the second hurdle or stage is not relevant. If the personal data is a special category of data, for example, data concerning health, you must consider the second stage.

Second stage
If the personal data is a special category of personal data and it may not be processed unless permitted by the GDPR and subject to any conditions in the GDPR.

Data concerning health may be processed – according to Article 9 (h) but the condition is that a professional subject to the obligation of confidentiality, such as pharmacist or pharmacy technician, must be responsible for a pharmacy company's processing of that data concerning health.

12. **Must all personal data be processed lawfully under one of the provisions in Article 6 of the GDPR and, if a special category of personal data, the processing be permitted in Article 9 of the GDPR?**

Yes.

Consent

13. Is consent still important?

Yes, but its use for the processing of data is not encouraged unless it is meaningful. Seeking consent for processing data associated with a prescription is not meaningful. Prescription data must be processed for a variety of reasons including patient safety, professional responsibilities, pharmacy payment and anti-fraud checks.

Patient consent or agreement (as a part of pharmacy practice) to the dispensing the prescription and, for example, consent to Medicines Use Reviews (MURs) and flu vaccinations remains as meaningful and important as ever, but once a patient has consented to this, generally records must be kept and often may be used by others caring for the patient. This is part of healthcare practice under the GDPR.

While consent for processing the personal data is not required, Privacy Notices explaining to patients what personal data is processed and for what purpose are necessary.

14. If I want to collect personal data by consent or I do already, how do I comply with the GDPR?

If you want to collect data by consent, there are stricter rules on the meaning of consent and how it should be obtained. The GDPR seeks to make any consent sufficiently specific to be meaningful and introduces an additional concept of explicit consent for consent related to special category personal data.

By 25th May 2018, all consent must comply with the new meaning of consent set out in the GDPR (must be GDPR compliant consent) and you must have a record of that GDPR compliant consent. If you have this already, you do not need to renew the 'consents' you have, for implementation of the GDPR. **If you do not have GDPR compliant consent, or do not have a record of this, you will have to renew the consent given before 25th May 2018 so that you have both.**

So, if the pharmacy has a separate marketing list for a specific purpose, to which those persons listed have given their consent, you may have to renew each person's consent before 25th May 2018 so that the consent is GDPR compliant and you have a record of it.

15. What is GDPR compliant consent?

The key point here is that generally you will not be processing personal data based on 'consent' in GDPR terms, but if you do, the data subject's **consent** is required for processing under Article 6; and the data subject's **explicit consent** is required for processing special categories of personal data, such as data concerning health (Article 9).

'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Consent gained by pre-ticked consent boxes is not valid consent under the GDPR.

Explicit consent is intended to be more specific consent, and must be confirmed in words, rather than by any other positive action i.e. the person giving consent must signal agreement to an explicit statement in words such as 'I consent to emails about your products and special offers'.

Broadly if personal data is collected by consent a data subject should be able to withdraw his or her consent at any time. Also, it should be as easy to withdraw consent as it was to give it.

Whether consent was freely given will depend on whether the data subject could give or refuse consent to the processing of data and still continue with the rest of the service or contract. If the data subject can do so, it is more likely that consent was freely given. If not, the data is processed, for example, by virtue of the contract only and should only be processed to the extent required by the contract.

If you collect personal data for marketing purposes, we advise you to read the guidance on consent by the Information Commissioner's Office.

16. Can I dispense and processes prescriptions without consent?

Generally, you need the consent or agreement of the patient to dispense that patient's prescription.

Generally, you do not need that patient's consent to process the data associated with the prescription (to which consent or agreement to dispense the prescription has been given).

Children's data

17. What about processing children's data?

For pharmacies dealing with prescriptions for children, normal professional rules and legal principles apply, and the GDPR should not add any additional requirements to those described elsewhere in these information booklets.

For those providing 'information society services' (services at a distance e.g. via the internet), which are generally for remuneration, and where the lawful processing under the GDPR is consent (Article 6(1)(a)), the GDPR sets out additional requirements. Broadly, to process personal data for any child below the age of 13 (for the UK), as an "information society service" you must have the consent of the person who holds parental responsibility for the child or have taken reasonable efforts to verify such consent.

Where services are offered direct to a child, you must ensure your Privacy Notice is written in a clear, plain way that a child will understand.

Data Protection Impact Assessments

18. Do I need to do a data protection impact assessment?

You may need to undertake a data protection impact assessment under the GDPR.

This should be reviewed at least when there is a change of processing operation.

19. What information should a data protection impact assessment (DPIA) include?

A DPIA should include:

a) a description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller;
b) an assessment of the necessity and proportionality of the processing in relation to the purpose;
c) an assessment of the risks to individuals;
d) the measures in place to address risk, including security and to demonstrate that you comply;
e) unmitigated risks (uncontrolled) have been identified and notified to the ICO; and
f) a DPIA can address more than one project.

(Question and answer is taken from the ICO website.)

20. What must I do if the data protection impact assessment indicates there is a high risk to the processing of personal data?

If there are high risks that personal data may not be protected – a high risk to the rights and freedoms of individuals – advice should be sought from the supervisory authority for the UK, the ICO.

Pseudonymised personal data

21. What is pseudonymised data?

Pseudonymised data is personal data that can no longer be attributed to a specific natural person without the use of additional information. Prior to the GDPR this might have been called anonymised data. Anonymised data is data where data subjects cannot be identified even with additional information, for example, statistical information. The processing of pseudonymised data is encouraged (with the key or patient names relating to that data held separately and securely) to improve the protection of data subjects.

22. What if I process pseudonymised personal data – personal data that does not identify the data subject and do not have details of the data subjects?

If you process pseudonymised personal data – personal data that does not identify the data subject but where the data subject could be identified later when the information is matched up with other information – and you do not have access to details of the data subject (the key or patient names), you are not required to acquire or process additional information in order to identify the data subjects and the data subjects do not have most of the rights to access or rectify data.

Security and personal data breaches

23. What must I do to process personal data securely?

To process personal data securely you must:

a) consider pseudonymisation and encryption of personal data (for some time it has been necessary to encrypt personal data held on laptops and memory sticks);
b) be able to ensure the confidentiality, integrity, availability and resilience of the processing systems and services;
c) be able to restore the personal data in a timely manner in the event of physical or technical problems; and
d) have a system for regularly testing, assessing and evaluating the effectiveness of the security, technical and organizational; recognizing the risks involved in processing the personal data, including the risk of unauthorised disclosure.

Any natural person processing personal data – for the data controller or the processor – does so under instructions from the data controller, the pharmacy business.

24. What is a data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

25. What do I do if there is a data breach?

You must document any personal data breaches, including the facts of the breach, the effects of the breach and any remedial action taken. The ICO may use these reports to assess compliance with the GDPR.

26. When must I notify a personal data breach?

Any personal data breach must be notified to the ICO within 72 hours of the data controller having become aware of it, **unless** the personal data breach is **unlikely** to result in a risk to the rights and freedoms of natural persons.

If the breach is reported later, the reason for the delay must be explained at the same time the breach is notified late.

27. What must I do to notify a personal data breach?

Breach notifications to the ICO must:

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
b) communicate the name and contact details of the DPO or other contact point where more information can be obtained;
c) describe the likely consequences of the personal data breach; and

d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

28. Will I be fined if there is a data breach?

The ICO has other enforcement powers such as warnings and reprimands and powers to ensure appropriate standards are met; it does have the power to fine and the fines under the GDPR are higher than before, up to 10 million Euros or 2% of global turnover. The maximum fine for non-compliance with an order by the supervisory authority, the ICO is double these amounts to 20 million Euros or 4% of total worldwide annual turnover.

Generally, regulators initially seek to encourage compliance with new regulations and rules, even after the date they apply, rather than enforcement action such as fine, provided that you are making efforts to comply with the new regulations and rules. It may be that this will be the ICO's approach.

The Data Protection Officer

29. Who is the Data Protection Officer (DPO)?

The DPO is a designated role under the GDPR which is intended to be given to somebody with expertise in data protection and who is both independent in decision-making – such as a professional – and senior in the organisation, who advises the organisation on data protection and GDPR issues. Guidance may be found in the Information Governance Alliance's guidance '*The GDPR Data Protection Officer*' at https://www.digital.nhs.uk/article/1414/General-Data-Protection-Regulation-guidance .

30. Do I need a DPO?

Maybe. There are two reasons why you might be required to have a DPO.

The first is because NHS pharmacies are subject to the Freedom of Information Act and any organisation that is subject to this Act is automatically deemed to be a public authority by the proposed data protection legislation accompanying the introduction of the GDPR.

If this remains the case all community pharmacies will need to appoint a DPO.

The second is because you may be considered to be a data controller '*processing on a large scale... special categories of data pursuant to Article 9* (which includes data concerning health).

Recital 91 in the GDPR (these are the preambles to the GDPR), albeit referring to data protection impact assessments (DPIAs) states:

> *…The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.*

Although, it is clear that 'processing of patient data in the regular course of business by a hospital is considered to be large-scale (Guidelines on Data Protection Officers ('DPOs'), Adopted on 13 December 2016, last Revised and Adopted on 5 April 2017).

If large-scale is the only basis for appointing a DPO this will only apply to community pharmacy business that can be described as large-scale.

We are seeking clarification of the DPO role and its applicability and must await the final form of the Data Protection Act 2018.

31. What is the position and role of the DPO?

The DPO is somebody who:

a) is appointed based on professional qualities and expert knowledge of data protection law;
b) may be a staff member or somebody external may be contracted to undertake the role; and
c) has a role liaising with the supervisory authority, the ICO – the DPO's details shall be published and communicated to the ICO.

The data controller and the processor need to:

a) ensure the DPO is involved properly and in a timely manner in all issues which relate to the protection of personal data;
b) support the DPO with the resources necessary to carry out the role and access to processing operations and so the DPO can maintain his or her expert knowledge;
c) ensure the DPO has the necessary freedom and protection to carry out the role without fear or favour;
d) ensure the DPO reports to the highest management level;
e) provide that data subjects may contact the DPO relating to issues on processing their personal data and their rights under GDPR;
f) bind the DPO to confidentiality; and
g) allow the DPO to carry out other duties and tasks (as appropriate) where there is no conflict of interest.

The DPO must have at least the following tasks:

a) inform and advise the controller or the processor and the employees who carry out processing obligations under the GDPR or other data protection provisions;
b) monitor compliance with the GDPR, considering data controller's policies, assignment of responsibilities, awareness-raising and training of staff involved in processing and related audits;
c) provide advice where requested on the data protection impact assessment and monitor its performance;
d) cooperate with, and act as a contact point for, the supervisory authority, the Information Commissioners Office; and
e) have due regard to the risks associated with processing operations in the performance of his role, taking into account the nature, scope, context and purposes of processing.

Privacy Notices – information to be provided to data subjects

32. What is a Privacy Notice?

The GDPR requires data controllers to provide to data subjects information about their processing and related matters and the rights of the data subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

33. What information must I provide to data subjects? (Privacy Notices)

Where the personal data is provided by the data subject, for example, when a prescription is presented to a pharmacy in hard copy or following EPS nomination of that pharmacy, the following information must be provided to the data subject (i.e. the patient):

a) the name and address of the data controller, the pharmacy company;
b) the contact details of the DPO;
c) the purposes for which the personal data is processed and the legal basis for this;
d) the recipients or categories of the recipients of the personal data, if any;
e) any relevant information about transfers to a third country or international organisation;
f) the period or criteria that will determine, how long the personal data is stored;
g) the relevant rights the data subject has in this case;
h) if the processing is based on consent, the right to withdraw that consent at any time;
i) the right to lodge a complaint with the supervisory authority, the ICO;
j) if the provision of personal data is a statutory requirement, the possible consequences of failure to provide it;
k) relevant information on automated decision-making; and
l) any processing of the information subsequently for a different purpose.

You do not need to provide this information if it has been provided to the data subject already.

34. How must this information be provided?

The information may be provided in writing or, at the request of the data subject, orally. Providing information may be by means of a notice in the pharmacy or on the website, whichever is more appropriate and may make use of standardised icons (which must be machine readable if provided electronically), to make the Privacy Notice easily visible, intelligible and the information clearer.

35. When shall I provide the information – the Privacy Notice – to a patient?

Ideally, the information in the Privacy Notice should be provided to a patient at the time the patient nominates the pharmacy for the dispensing of its prescriptions, but it could be provided when the first prescription is dispensed.

The information could be provided by way of an information notice on the wall of the pharmacy that is visible to patients, or electronically on a website if appropriate, and it is

suggested that a patient's attention is drawn to the Privacy Notice when the pharmacy dispenses the patient's first prescription, or subsequently when the notice is first displayed.

The notice could be handed out to the patient or included in the bag of dispensed medicines, when a patient's first prescription at the pharmacy is dispensed; or included in the pharmacy leaflet required for NHS pharmacies.

36. Are there special rules if the information is not provided to the pharmacy by the patient?

Yes. There are additional rules if the personal data has not been supplied by the pharmacy, but generally a pharmacy will be able to provide the required information when, for example, the prescription is dispensed. Further information is provided by the ICO.

Health and Employment data

37. Can I process health data and employment data without consent?

Yes. Health data may be processed by a pharmacy on the basis, for example, that it is necessary for the performance of a task carried out in the public interest (Article 6, 1(e)); or processing is necessary for compliance with a legal obligation (the Terms of Service in the NHS (Pharmaceutical and Local Pharmaceutical Services) Regulations 2013) (Article 6(c)). There will also be many occasions when health data in a pharmacy is processed to protect the vital interests of the patient (Article 6(d)). As health data is a special category of personal data, the second stage of lawful processing must also be considered. (See question 10)

Employment data may be processed lawfully under one or more of the broad categories in Article 6, for example, as necessary for the performance of a contract and, for tax and national insurance purposes, for compliance with a legal obligation. It is generally not special category data and, therefore, Article 9 need not be considered.

Processors

38. What are processors, and can I send my staff's data to a third party for payroll purposes?

Processors are those people to whom you send personal data for a specific task, who you instruct exactly what to do with the personal data, for example, when you send information to a third-party organisation for your payroll.

39. What must I agree with my processors?

You must have a contract or other legal provision which ensures they are GDPR compliant and if they are not in the UK, additional requirements may apply.

The ICO indicates that contracts with processors:

Must set out:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the obligations and rights of the controller.

Must also include as a minimum the following terms requiring the processor to:

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

Processors may not pass the personal information to a third party – another processor – without prior written authorisation from the data controller; and if this is permitted the contract with the additional processor must include the same data protection requirements as the original contract.

Data subject rights

40. What do I have to provide or do at the request of the data subject?

Data subjects had various rights under the Data Protection Act 1998 and broadly these rights remain and are developed and clarified under the GDPR. Some rights only apply to personal data which is collected by consent, on the basis that if you consent to the collection of data you ought to be able to retract that consent. The key rights that data subjects have are as follows and those highlighted are the most significant for community pharmacy:

a) Right of access – data subjects have a right to obtain from you a copy of the personal data you hold on them (e.g. from the PMR), free of charge on the first occasion, and the following information

i) Purpose of the processing
ii) Categories of personal data concerned
iii) To whom you disclose the data
iv) How long the data is stored or how this is calculated
v) The existence of the right to rectification or reassure (not erasure for health data)
vi) Right to lodge a complaint with the ICO
vii) If not collected from the data subject, where the personal information came from
viii) Additional information related to automated decision-making and transfer of personal data overseas)

b) Right to rectification – the data subject may ask for incorrect or inaccurate information to be corrected, which may be more appropriate by way of a supplementary statement, because, for example, the record of what was prescribed or dispensed may need to be retained for professional or legal reasons.

c) Right to erasure – particularly relevant if the only ground for processing personal data is consent (or explicit consent if the information is special category personal data). The right to erasure does not usually apply to data concerning health processed for healthcare and NHS management purposes.

d) Right to restrict processing – in some cases the data subject may restrict your normal processing and may, for example, ask you not to delete data you would otherwise delete, because the data subject needs the data for a legal case.

e) Right to have others notified of any rectification, erasure or restriction - any rectification, erasure or restriction must be notified to each person to whom the data has been disclosed unless this proves impossible or would involve a disproportionate effort.

f) Right to data portability – this applies only where the processing is based on consent or a contract (and therefore in most cases should not apply to data concerning health)

g) Right to object – which could apply to pharmacies – in which case the pharmacy should provide a copy of the Privacy Notice and will need to show for each specific case that it has compelling legitimate grounds for processing the personal data that

overrides the interest, rights and freedoms of the data subject; or the pharmacy may retain the data for the establishment, exercise or defence of legal claims.

Data subjects will not be able to exercise all the rights in relation to pharmacy – see step 11 in the **Guidance for Community Pharmacy** (Part 1).

41. When do I have to provide relevant information to data subjects?

You must provide relevant information to the data subject without undue delay and in any event within **one month** of receipt of the request. If you need more time you need to tell the data subject and explain why. If you have not taken the action requested you should provide the details of the supervisory authority, the ICO, so the data subject may lodge a complaint.

42. How should I provide the information?

If the information is requested electronically, it should be provided electronically, if possible, unless otherwise requested by the data subject.

43. Can I charge a fee for providing information to data subjects in response to these requests?

No. Unless the request is manifestly unfounded or excessive, for example, because they are repetitive, in which case you can charge a reasonable fee or refuse to act on the request.

44. Can I refuse these requests from data subjects?

Yes, but only in certain cases, see the answer to the question above.

45. May I check the identity of the data subject?

You may, and you should, to ensure that you do not disclose confidential information to the wrong person.

Data protection by design and default and DPOs

46. Do I have to think about data protection by design and default?

Yes. Designing systems and procedures with recognition of data protection principle has long been important and it is now a requirement of the GDPR. There is also a requirement in certain cases to appoint a DPO. This requirement is intended for public authorities but by a quirk of legislation may apply to community pharmacies as well. (See earlier DPO section)

Cooperating with the Supervisory Authority – the Information Commissioner's Office (ICO)

47. Do I need to continue to pay an annual fee to the ICO?

Yes, you must continue to pay an annual fee to the ICO.

48. Do I need to cooperate with the ICO?

Yes, the ICO is the relevant supervisory authority for the UK and enforces data protection rules, regulations and legislation. Data controllers and processors must cooperate with the ICO.

The ICO also provides extensive guidance on data protection and the GDPR.